Configuration Management Plan
for
US Department of Energy
Headquarters

DRAFT

Associate CIO for Operations (MA-44)
US Department of Energy
June 1999

Table of Contents

1 Introduction

1.1. Purpose

This Configuration Management Plan (CMP) establishes the overall plan to be used by all organizations within Headquarters, US Department of Energy (Washington, DC and Germantown, MD) for Configuration Management during all life cycle phases of all information technology systems, assets and infrastructure used at headquarters. The CMP generally follows, but does not necessarily comply fully, with the technical standards set by the MIL-STD-973 Configuration Management and other commercial standards, as they apply to DOE Headquarters. It is written at a headquarters, cross-project and cross-system level to establish policies, standards, procedures, and uniform practices for configuration management of all computer software, hardware, and local and wide area network communication resources and associated documentation and drawings.

1.2. Scope

The purpose of Configuration Management is to maintain the integrity of products and systems as they evolve from specifications through design, development, installation and production. Configuration management is not an isolated endeavor; it exists to support product development, use and maintenance.

This plan applies to all hardware, drawings, documentation, computer programs, tools and processes used in the production of all systems for DOE Headquarters. This plan includes all phases of the development life cycle. The following headquarters organizations, referred to elsewhere in this document as "participating organizations," are included under this CMP:

- Office of the CIO, Operations Division (MA)
- Defense Programs (DP)
- Office of Science (SC)
- Environment Management (EM)
- Energy Efficiency (EE)
- Environment, Safety & Health (EH)
- Fossil Energy (FE)
- Nuclear Energy (NE)
- Civilian & Radioactive Waste (RW)
- Other Program Offices

The CMP is a living document and as a result additions, deletions, and modifications will occur as it is utilized. It will be updated as additional configuration activities are defined as the work proceeds and the necessity arises. Therefore, to provide configuration identification, this CMP document will be identified with an issue or version number and will itself be maintained under configuration control.

1.3. Background

A Headquarters Configuration Control Board and process needs to be established to allow for more compatibility and interoperability of information technology infrastructures and to ensure compliance with Departmental Information Architecture concepts. It is becoming increasingly difficult to implement new information systems and technical infrastructures or changes to existing systems in the existing Headquarters environment. More collaborative effort on mutual needs is necessary to provide the communications and telecommunications networking within and across organizations, as well as Department wide, to meet mission needs as cost effectively as possible.

The Headquarters configuration control process and CCB will be established to oversee the management of changes for all Headquarters information technology infrastructures. The CCB is not a funding vehicle. It provides approval for making changes to keep systems safe and operational. It will not preclude the establishment of individual configuration control processes nor development of individual configuration management plans within Headquarters organizations.

The configuration control process is not an administrative process, but a binding approval process that must be followed to handle the concerns that are currently faced. The ultimate goal in this regard is to operate safely and to not adversely affect the operation of other organizations.

2 RESOURCES AND ORGANIZATION

This section describes and graphically portrays the organization with emphasis on the Configuration Management (CM) activities, and will include:

a. The relationships and integration of the project organization and functional organization;
b. Responsibility and authority for CM of all participating groups and organizations including their role in configuration control boards, and the integration of CM functions with other program activities such as technical reviews;
c. Identification of the project's CM organization and its responsibilities; and
d. Interfaces between the project's CM organization and the subcontractors, and associate contractors.

2.1 Organizational Structure

The Associate Chief Information Officer for Operations (MA-44) is the Headquarters Configuration Manager, and has total responsibility for overall configuration management for DOE Headquarters. As part of the planning effort, this configuration management plan has been produced to provide overall policy and planning guidance for configuration management throughout this project. A Configuration Management Coordinator (CMC) will

be designated by the Configuration Manager from among the personnel resources available from the MA44 team, and will be responsible for implementation of this plan. Figure 2.1.1 depicts a generic Configuration Control Board structure for DOE Headquarters. The line management of each supporting organization is responsible for insuring that configuration management procedures are followed within their organizations.   Each Program Office will have their own designated CM to interface with the Headquarters CM.

Figure 2.1-1 DOE Headquarters CM Organization Chart
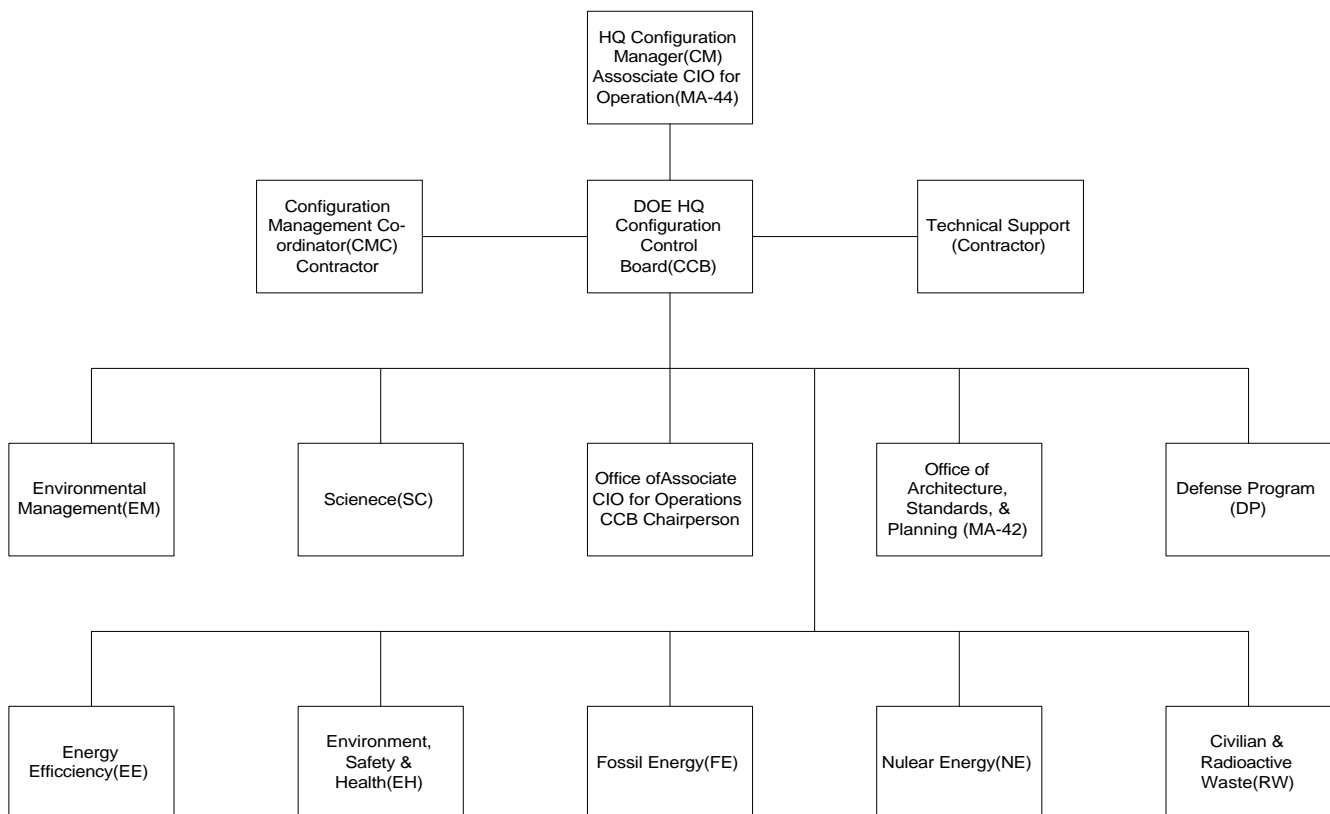
2.2   *Relationship Between the CM Office and Supporting Organizations*

System Change Proposals that affect substantial project milestones (schedule, budget, etc.) or that affect interfaces between systems and subsystems (normally controlled by Interface Control documents, or ICD's) between supporting organizations are the responsibility of the DOE Headquarters Configuration Control Board (CCB). System Change Proposals that do

not affect other organizations or headquarters policies, schedules or budget are to be evaluated at the lowest level practical. It is incumbent upon each organization at headquarters to fully understand the impact of possible changes and to refer any requests that may have ramifications to ICD's or the headquarters infrastructure as a whole up the CCB.

Each organization is required to utilize appropriate levels of configuration management in support of the Headquarters CM. Management of each participating organization will act as, or designate, its own Configuration Manager. The Configuration Manager will have full authority to evaluate configuration System Change Proposals for its own organization, implement necessary documentation procedures, and evaluate the impact of System Change Proposals.

It is to be expected that each participating organization will have customers and processes external to the HQ CM Office, and will have existing CM processes in effect. Existing processes and procedures will be employed in support of the headquarters CM where possible and additional processes will be required where necessary to insure the functionality of the overall Configuration Management Plan. Additional processes may include the addition of identification of Change Status, Change Effectiveness, etc. to existing forms, for example, in order to enable the HQ CCB to fully evaluate CI System Change Proposals, impacts, etc. Where processes at the participating organization do not enable HQ CM to control and monitor CI's, additional process implementation will be requested by the HQ CM organization.

3   Referenced Documents

The following specifications, standards, manuals and handbooks form a part of this document to the extent specified herein.
> [1] MIL-STD-973, Configuration Management, April 17, 1992

4   Configuration identification

Configuration identification, in general, provides the means by which the performance, qualification, fabrication, and acceptance requirements associated with the product under development are progressively defined, documented, and placed under control.

4.1   Baseline Identification

Using appropriate technical documents (including specifications, drawings, computer software listings, and part lists), the configuration identification process establishes baselines with more detailed descriptions of the functional and physical characteristics of the items. The baselines are established by the Configuration Control Board (CCB), with the technical assistance of the MA44 team and the participating organizations' Configuration Managers, at points in the program where it is deemed necessary to provide a definable and manageable departure point for the development and production of the system or individual item(s). For

instance, departures from the baseline are possible specific business needs of participating organizations. The baseline, plus any approved changes to it, constitutes the current binding configuration identification (that is, the technical definition of what the system/item is expected to accomplish). By establishing baselines, the orderly development of the system from specifications into design documentation, and then into the hardware and software items, is possible. When the configuration items are baselined, the Headquarters Configuration Control Board (CCB) must approve any changes to the configuration.

At Headquarters, baselines for the different systems and configuration items are established when the system has completed the Critical Design Review (CDR) process. The CDR process will insure:

- Acceptance of basic design approach
- Compliance with project requirements
- Definition of Interface Requirements (Interface Control Documents)
- Maintainability/Reliability
- Usability
- Test Planning
- Safety Assessments, if relevant
- Release of detailed design
- Acceptance Test Requirements

Upon completion of the CDR process, the system design will have been finalized, and any further changes must be approved by the Configuration Control Board. It is the responsibility of the participating organization's Configuration Manager to submit a list of configuration items for their system design to the CMC for inclusion into the configuration control process. It is also the responsibility of the participating organization's Configuration Manager to insure that no changes are allowed in the system design once the design has been baselined.

4.2   Configuration Items

Since a project or subsystem consists of different facilities with functionally similar hardware and software, there will be a unique numbering system that provides some uniformity among the facilities. The identification of configuration items must allow the project to control and have traceability between the different facilities of the project. A complete list of configuration items that will be placed under configuration management will be maintained by the CMC. It will be the responsibility of the CMC to insure a consistent numbering scheme for the configuration items.

4.2.1   Hardware

The hardware for Headquarters will be divided (at a minimum) into the following categories: desktops, servers, peripherals, network devices (routers, switches, etc.). Hardware Configuration Items may include requirement documents, design documents, schematics, hardware manuals, end-user documents, and the actual physical parts. An identification number consisting of a part number, serial number, and/or drawing number will identify all hardware parts and assemblies. Methods used to identify hardware such as engraving, ink

markings, or tags will be compatible with hardware being labeled. A system of subsidiary CI's which constitute higher-level CI's should be implemented if warranted.

4.2.2   Software

The software for Headquarters will be divided into the following categories: operating systems, COTS application software, network operating systems, and other communication software. Each Software Configuration Item will be assigned a unique code.

4.2.3   Communication Circuits

Communication circuits for Headquarters will be divided into the following categories: wide-area circuits and local-area network elements.   Each Communication Circuit Configuration Item will be assigned a unique code.

4.2.4   Documents

This section establishes the policy and procedures for identifying documents specifically controlled by the CM process. At a minimum, Requirements Documents, Interface Control Documents, Quality Assurance Plans, and meeting minutes will be under configuration control and numbered using a standardized numbering scheme. Documents will be maintained in hard-copy and electronic format as available in a configuration management library managed by the MA44 team. Documents, numbers and changes to documents will be issued and validated by the CMC.

4.2.5   Drawings

Drawings may be categorized according to their source: In-house-developed drawings, or contractor/vendor supplied drawings. In-house-developed drawings will normally be formatted and numbered according to the standards noted above. Contractor-developed drawings (unless specified otherwise by contract) will normally be delivered using the contractor's format and numbering scheme. Each participating organization's Configuration Manager will designate a responsible individual or individuals to keep track of drawings and numbers and to maintain currency, and to transmit appropriate information to the central CM library catalog. The designated individual will be responsible for coordinating changes and updates with Configuration Management Coordinator (CMC).

4.3   *Document Tree*

A Headquarters CM Document Tree will be developed to catalog high-level requirements, detailed derived requirements, the configuration items, and interface control documents. The Document Tree will be maintained by the CMC. Figure 4.2-1 shows a sample document tree. The system is decomposed into subsystems, and further into hardware and software configuration items. The top-level design of the hardware/software configuration items is documented in hardware/software design documents, while the lower levels of the design are carried forth into engineering drawings/behavioral diagrams. Each level of decomposition (system, subsystem, and configuration item) may contain its own test plans, test procedures, and test reports as necessary.

```
Project Specification
|
| -- High-level Plans / Requirements / Procedures / Reports
|
| -- Operator and Maintenance Manuals
|
| -- Subsystem Specifications
|
| -- Derived Plans / Requirements / Procedures / Reports
|
| -- Interface Control Documents
| |
| | -- Configuration Items
| | |
| | | -- Hardware
| | |
| | | -- Software
| | |
| | | -- Network Segments
etc.
```

Figure 4.3-1 Sample Document Tree

5   CONFIGURATION CONTROL

Configuration control assists in maintaining the integrity of the system by maintaining cognizance of all changes to baselined configuration items under the configuration control process.

5.1   Headquarters Configuration Control Board

The various participating organizations (e.g. DP, etc.) and contractors are subsidiary organizations with respect to the Headquarters CCB, and will undertake configuration management of non-common hardware and software, items that have no impact on interfaces, schedule, milestones, etc. All changes to baselined CI's are submitted to the Headquarters CCB using a System Change Proposal (SCP) form. CCB is responsible for assessing the impact of proposed changes to baselined CI's and for approval/disapproval of the proposed changes. The CCB is chaired by the Configuration Manager (i.e. Associate CIO for Operations, MA-44) or his/her designee, and is supported technically and administratively by the MA44 contractor.

5.1.1   Participating Organization Configuration Control

Each participating organization is responsible for establishing/maintaining an acceptable CM process for items which do not affect interfaces, schedule, milestones or other critical issues at the Headquarters level. CM at this level may be performed via a standing CCB board or other formal process. A participating organization's Configuration Management Coordinator (CMC) will be designated to develop/modify CM processes, provide interface Point of Contact to other organizations, to evaluate impacts of System Change Proposals, and to represent the participating organization to the Headquarters CCB.

5.1.2   Headquarters CCB Membership

CCB membership consists of all Headquarters IT Collaboration Group elements affected by any proposed change(s). Depending upon the magnitude of the change, this can be a single organization or multiple organizations. In addition to the Chair and representatives of the Collaboration Group, at the discretion and invitation of the Chair, representatives from the following functions should also be CCB members:

- Financial/Budget
- Procurement
- Security
- Integration/Architecture

Voting members will consist of the CCB Chair, the three Lead Program Secretarial members and five other Program Office members of the Headquarters IT Collaboration Group, as follows:

- CIO/OPS
- DP
- EE
- EH
- EM

- FE
- NE
- RW
- SC

5.1.3   Headquarters CCB Process

To run a CCB efficiently, the following are desirable:
   a.   A written published project instruction that establishes the board, states the scope of the boards' activities, and identifies the standing, non-voting members.
   b.   Regularly scheduled meetings at a fixed time and place. Any interested party may attend.
   c.   An agenda should be published well in advance of the meeting, with all items (e.g., SCP's) to be covered at the meeting. The goal is to enable the individuals involved to review the material in depth prior to the meeting, and thus to have an opportunity to raise their concerns.
   d.   The secretary and chair. The secretary ensures that the paperwork is distributed in a timely manner, including the agendas, minutes of the previous meeting, and the material to be considered as part of the next meeting. The chair is ultimately responsible for configuration decisions. For the DOE Headquarters CCB, the CMC or other representative from the MA44 contractor will serve as the CCB secretary. The Associate CIO for Operations (MA-44) or designee will be the chair.

5.2   System Change Proposal Form

Headquarters will implement a standard System Change Proposal (SCP) form. The SCP will be accessible either electronically or by hardcopy by contacting the CMC. The SCP should be used for requesting changes to any facilities associated with the system. At the participating organization level, existing CM System Change Proposal processes may be used. Figure 5.2-1 illustrates the Configuration Control Process.

5.2.1   Requesting Changes

Any changes that will modify a baselined CI will be documented by a SCP form and be processed by the CCB. Hardware, software, network elements, documents, and drawings associated with a system design are considered baselined after a completed CDR process, therefore any changes beyond the CDR will require a SCP form. The SCP form is submitted only against baselined CI's.

Changes to any of the CI's may be initiated by members at the Headquarters level, supporting participating organizations, or members of the MA44 organization. The SCP may be a new requirement, an enhancement/modification, or a defect correction. Refer to Appendix C for the SCP form. The initiator of the change and the participating organization Configuration Manager or CMC will complete appropriate parts of the SCP form. The participating organization Configuration Manager or CMC should ensure that the SCP has enough information to verify the reported defect or test the requested enhancement or requirement and then pass the SCP form to the secretary of the CCB. The secretary assigns a SCP number and the SCP is passed directly to the CCB to be reviewed.

5.2.2   Evaluating Changes

The receiving CMC will review the SCP form and assess whether the change affects software, hardware, or both, with related drawings and documentation. This information is then submitted to the CCB chair for approval. The CCB chair may submit the SCP to the technical staff of the MA44 organization for technical evaluation and review, including bench tests of compatibility or suitability, as the situation warrants.   The MA44 organization will prepare evaluation results for the review of the CCB and the chair.

5.2.3   Approving or Disapproving Changes

The CCB chair will review the information provided to determine whether the change will be approved. The chairperson may contact the initiator for suggested modifications to the SCP form before accepting the request. The chair may also initiate an agenda item at a forthcoming CCB meeting to discuss and vote upon the proposed change, under the CCB charter. If the SCP is approved, the CCB chairperson will assign its priority level and submit it to the proper manager(s) for implementation. The CCB may reject the request and provide a reason for the rejection. A rejected SCP is considered closed. The CCB may also partially reject a CCB and return it to the originator for update or revision. Following acceptance or rejection, the initiator will receive a notification on the status of the SCP. An informational copy of any action taken by a participating organization's CCB will be forwarded to the chair and other CCB members.
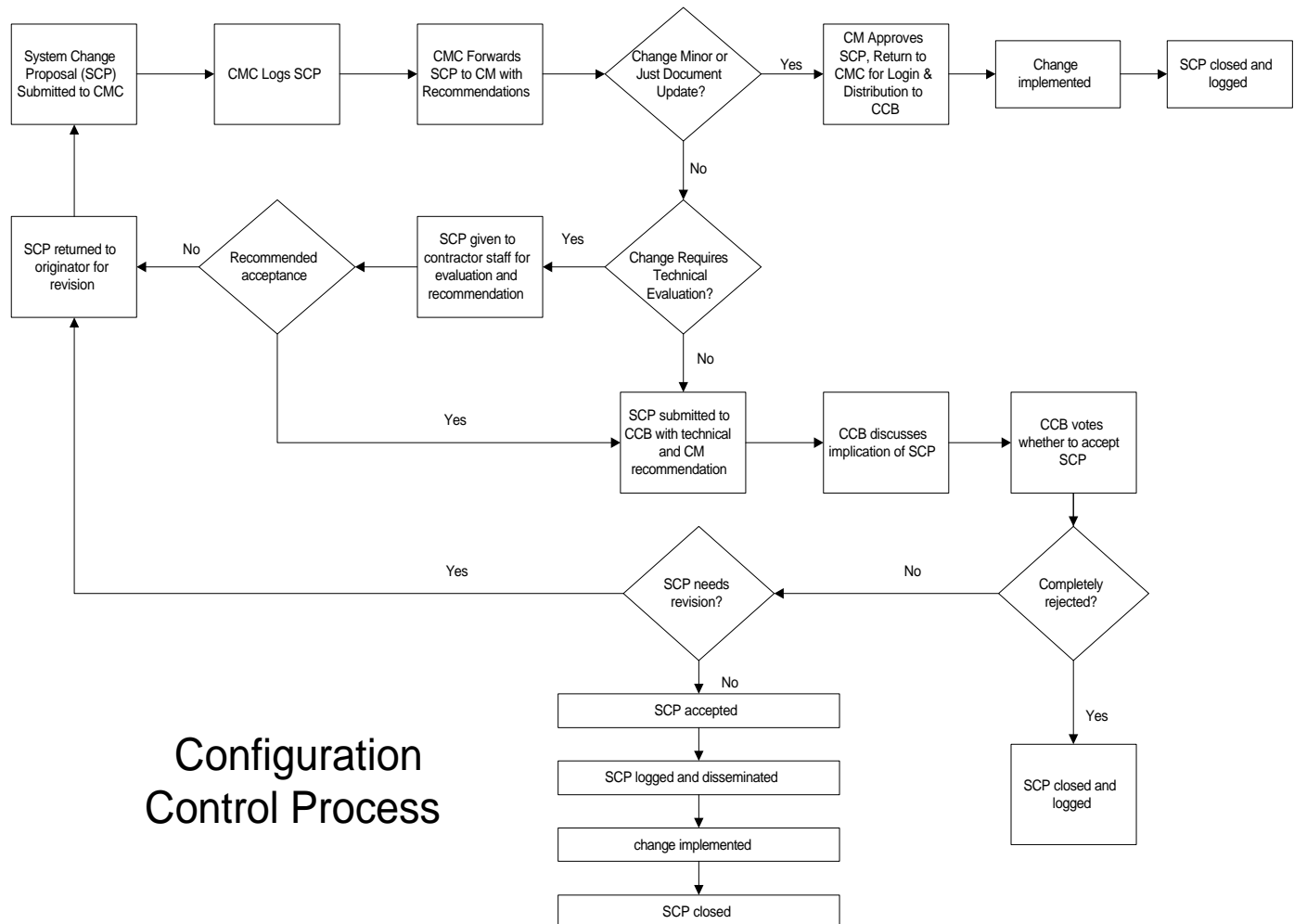
System Change Proposal (SCP) Submitted to CMC → CMC Logs SCP → CMC Forwards SCP to CM with Recommendations → Change Minor or Just Document Update?

Change Minor or Just Document Update? — Yes → CM Approves SCP, Return to CMC for Login & Distribution to CCB → Change implemented → SCP closed and logged

Change Minor or Just Document Update? — No → Change Requires Technical Evaluation?

Change Requires Technical Evaluation? — Yes → SCP given to contractor staff for evaluation and recommendation → Recommended acceptance

Recommended acceptance — No → SCP returned to originator for revision → System Change Proposal (SCP) Submitted to CMC

Recommended acceptance — Yes → SCP submitted to CCB with technical and CM recommendation

Change Requires Technical Evaluation? — No → SCP submitted to CCB with technical and CM recommendation → CCB discusses implication of SCP → CCB votes whether to accept SCP → Completely rejected?

Completely rejected? — No → SCP needs revision?

Completely rejected? — Yes → SCP closed and logged

SCP needs revision? — Yes → SCP returned to originator for revision

SCP needs revision? — No → SCP accepted → SCP logged and disseminated → change implemented → SCP closed

Configuration Control Process

Figure 5.2-1 Configuration Control Process

5.2.4 Implementing Changes

The participating organization Configuration Manager(s) will work together, and with the chair, to ensure that appropriate procedures are followed and that no changes will have unforeseen impacts on other organizations or Headquarters as a whole. All changes to approved baselines will be implemented through the use of existing mechanisms, depending on the type of change

For items reviewed at the CCB, the participating organization Configuration Manager is granted change authorization only when he/she receives an approved SCP. For items reviewed within the participating organization, the participating organization CM authorizes the System Change Proposal. With respect to any change authorization (at either level), in order to guard against the introduction of new defects into the baseline system,

implementation of a change is not complete until the documentation has been updated and the change has been fully tested. The responsible individual will then fill out a change report form (see Appendix C). The change must be verified by the participating organization Configuration Manager(s), who ensures the change is in place and is correct. The names and versions of the modified CI components (if any) will be recorded in the report. A copy of the Change Report will be forwarded to the CMC.

5.2.5   Closing the SCP

A rejected SCP is considered immediately closed and no further action is taken on it. The closure procedures for an approved request begin when the participating organization Configuration Manager receives the Change Report from the system designer.   The participating organization Configuration Manager will issue a report requesting that other project members verify the change (i.e. ensure that it does not produce any side effects to their current work). Upon verification, the participating organization Configuration Manager will make the change a permanent part of the current baseline. The CCB chair then signs off the SCP as closed, and the report is reissued to announce the incorporation of the change. The SCP initiator will then be notified that the SCP has been closed.

5.3   *Problem Reporting and Corrective Action System*

At Headquarters level, the problem reporting and corrective action system follows the same procedures previously identified for a change to a baselined item. Refer to the appropriate participating organization Configuration Manager for details of the problem reporting and corrective system for their subsystem.

5.4   *Waivers and Deviations*

At the Headquarters level, waivers and deviations follow the same procedures previously identified for a change to a baselined item. All waivers and deviations will be processed through the Associate CIO for Operations (MA-44).

6   CONFIGURATION STATUS ACCOUNTING

The Configuration Status Accounting system will be implemented by the CMC and will:
   a. Identify the current approved configuration documentation and identification number associated with each CI.
   b. Record and report the status of proposed engineering changes from initiation to final approval/contractual implementation.
   c. Record and report the results of configuration audits to include the status and final disposition of identified discrepancies.
   d. Record and report the status of all critical and major requests for deviations and waivers which affect the configuration of a CI.
   e. Record and report implementation status of authorized changes.

 f. Provide the traceability of all changes from the original baselined configuration documentation of each CI.

 g. Report the installation status of configuration changes to all CI's at all locations.

6.1 *Configuration System Reports*

The Headquarters configuration system is a database used to record and retrieve all configuration items and associated information. The items available from this system include:

1. A list of all the SCP forms and their status.
2. A list of all the baselined CI's to include documents, drawings, hardware and software.
3. The problem report status, which provides a list of open/closed problem reports.

6.2 *Configuration Status Accounting Report*

This is a formal report and provides the complete status of:

 a. The contract, including the statement of work and other contract documents
 b. The system specification and the other documents identified in the document tree
 c. The equipment planning diagrams
 d. Program plans
 e. Problem reports
 f. Proposed changes
 g. Implementation of approved changes

7 CONFIGURATION AUDITS

Configuration Audits are performed when requested by the Associate CIO for Operations (MA-44). Configuration Audits consist of the Functional Configuration Audit, the Physical Configuration Audit, and the in-process audit.

7.1 *Functional Configuration Audits*

The purpose of a functional configuration audit is to validate that the installation and implementation of a configuration item has been completed satisfactorily, and that the configuration item has achieved the performance and functional characteristics specified in the functional or allocated configuration.

7.2 *Physical Configuration Audits*

The scope of the physical configuration audit is as follows:

 a. The audit will be conducted on the hardware and the hardware component of firmware.
 b. The audit will be a comparison of the hardware to the documentation.

15

    c. The level of the audit is such that disassembly of the hardware will not be required, but removal of modular replaceable assemblies will be accomplished to make all assemblies for the audit visible.

8   ARCHIVING

Archiving of all CI's to include drawings, configuration management reports, configuration items listings, etc. will be the responsibility of, and controlled by, the CMC.

9   SUBCONTRACTOR/VENDOR CONTROL

All hardware and software supplied by outside suppliers will be subjected to these CM Plan requirements. For subcontractors, the participating organization provides requirements in a Statement of Work. The subcontractor conducts a Preliminary Design Review, a subsequent CDR, and delivers the product. For subcontractors/vendors at the Headquarters level, the MA44 organization will be responsible for including CM requirements in subcontracts and enforcing them with the suppliers.

APPENDIX A -- List of Acronyms

CCB	Configuration Control Board
CDR	Critical Design Review
CI	Configuration Item
CM	Configuration Management
CMC	Configuration Management Coordinator
CMP	Configuration Management Plan
SCP	System Change Proposal

APPENDIX B -- Glossary of Terminology

System Change Proposal (SCP) -- The form used to initiate a request for a change to the baseline.

Configuration Control -- The formal process used to assure order in making changes to the baseline. This change control is accomplished through formal configuration control boards.

Configuration Control Board (CCB) -- A board composed of technical and administrative representatives who recommend approval or disapproval of proposed engineering changes to a CI's current approved configuration documentation. The board also recommends approval or disapproval of proposed waivers and deviations from a CI's current approved configuration documentation.

Configuration Identification -- Includes the definition and establishment of the baseline plans, requirements and configuration items to be controlled.

Configuration Item (CI) -- An aggregation of hardware and/or software and related documentation that satisfies an end use function and is designated for separate configuration management by the program/project manager.

Configuration Management (CM) -- A formal and disciplined system for identifying, controlling, verifying and accounting the physical and functional characteristics (i.e., form, fit, and function) of an item to ensure that the final product is built and qualified to specification.

Configuration Management Plan (CMP) -- Defines the concepts, requirements, processes and data for implementing configuration management on a particular program/project in compliance with the requirements established by the program/project manager.

Configuration Status Accounting -- An on-going process of recording and reporting all information required to manage the configuration items effectively.

Deviation -- A specific written authorization, granted prior to the manufacture of an item, to depart from a particular requirement of an item's current approved configuration documentation for a specific number of units or a specified period of time.

Drawings -- Engineering documents which disclose by pictorial or textual presentation, or both, the physical and functional requirements of an item.

Functional Configuration Audit -- The formal examination of functional characteristics of a configuration item, prior to acceptance, to verify that the item has achieved the requirements.

Life Cycle -- The period of time that starts when a product is conceived and ends when the product is no longer available for use.

18

Physical Configuration Audit -- The formal examination of the "as-built" configuration of a configuration item against its technical documentation to establish or verify the configuration item's product baseline.

Request for Deviation / Waiver -- A change documentation form that must be submitted to the program review board or configuration control board for approval.

Waiver -- A written authorization to accept an item, which during manufacture, or having been submitted for acceptance, is found to depart from specified requirements, but nevertheless is considered suitable for use "as is" or after repair by an approved method.

APPENDIX C -- Configuration Management Concepts

Configuration management (CM) is the discipline of identifying all components and their relationships in a continually evolving system, taking into account relevant system interfaces, for the purpose of maintaining integrity, traceability and control over change throughout the life cycle. It is a disciplined process of technical and administrative direction and surveillance to the identification and documentation of a system's functional and physical design requirements, the management of subsequent changes and the verification of successful requirement implementation.

CM comprises four major elements, more fully defined below:

- Configuration identification: Identifying and documenting the functional and physical characteristics of configuration items.
- Configuration control: Controlling changes to configuration items and their related documentation.
- Configuration auditing: Recording and reporting information needed to manage configuration items effectively, including the status of proposed changes and implementation status of approved changes.
- Status accounting: Auditing configuration items to verify conformance to specifications, drawings, interface control documents, and other contractual requirements.

Configuration Identification

Configuration Identification is the selection of the documents to comprise the baseline for the systems and configuration items (CI's) involved, and the numbers and other identifiers affixed to the items and documents. The identification of an item includes the approved documents that identify and define the item's functional and physical characteristics in the form of specifications, drawings, associated lists, interface control documents, and documents referenced therein. The configuration identification is developed and maintained through three distinct evolutionary increasing levels of detail; each is used for establishing a specific baseline. The three levels of configuration identification are as follows:

a. Functional Configuration Identification. FCI is the initial approved technical documentation for a CI which prescribes:
   (1) all necessary functional characteristics (i.e. functional requirements);
   (2) the verification required to demonstrate achievement of specified functional characteristics;
   (3) the necessary interface characteristics with associated CI's;
   (4) key functional characteristics and its key lower level CI, if any; and
   (5) design constraints.
b. Allocated Configuration Identification. ACI's are performance-oriented specifications governing the development of CI's, in which each specification:
   (1) defines the functional characteristics that are allocated from those of the system or higher level CI's,

(2) establishes the verification required to demonstrate achievement of its allocated functional characteristics,

(3) delineates necessary interface requirements with other associated CI's; and

(4) establishes design constraints, if any, such as component standardization, use of inventory items, and integrated logistic support requirements.

c. Product Configuration Identification. PCI is the current approved or conditionally approved technical documentation which defines the configuration of a CI during the production, operation, maintenance, and logistic support phases of its life-cycle, and which prescribes:

(1) all necessary physical or form, fit and function characteristics of a CI;

(2) the selected functional characteristics designated for production acceptance testing; and

(3) the production acceptance test requirements.

Configuration Control

Configuration control is the systematic proposal, justification, evaluation, coordination, approval or disapproval of proposed changes, and the implementation of all approved changes, in the configuration of a configuration item after establishment of the configuration baseline for the configuration item.

Configuration control provides the visibility and positive control of evolving hardware and software products. It is a formal change management process which controls all major changes that might affect the application and the distributed computing environment in which it operates. A proactive change-management process minimizes potential risks such as significant system outages or performance degradation, which adversely affect critical business operations. This change-management process typically involves designing a change-management business process, and assigning roles and responsibilities to individuals and organizations(for example, forming a configuration control board, or CCB, with technical representatives from each major group within an organization), as well as managing the ongoing operation of the change management business process.

Configuration control ensures that only customer approved changes are implemented after a formal baseline is established. It also provides the infrastructure needed to control software products and to manage the software development process. Typical changes managed under configuration control include::

- All system architecture changes
- All system interface changes
- All significant (i.e., other than minor clarifications or corrections) changes to the Functional Configuration Documentation
- All changes to the allocated Configuration Documentation or product Configuration Documentation that affect:
  a) System safety
  b) System performance
  c) System reliability
  d) System interface/interoperability characteristics.

Configuration Status Accounting

Configuration Status Accounting is the implementation of an information system that will provide timely, current, and accurate information that satisfies the evolving information needs of the using community. It is a process of maintaining an ongoing record of the status and history of all baseline configuration components, including:

    a) A record of the approved configuration documentation and identification numbers;
    b) The status of proposed changes, production permits and concessions to the configuration;
    c) The implementation status of approved changes, and
    d) The configuration of all units of the CI in the operational inventory.

Configuration Audits

Configuration audits ensure that all appropriate configuration items are properly identified, documented, and managed via a formal configuration and change-management process. There are two types of audit:

a) Functional Configuration Audit: The Functional Configuration Audit reviews system requirements and ensures that they have been qualified. Qualification can be accomplished by validation (i.e. software testing) or verification(e.g., inspection, audit, review).
b) Physical Configuration Audit: Physical Configuration Audit ensures the correlation of all hardware and software products before acceptance and before a product baseline established.

Appendix D   Configuration Management Control Board Charter

1. Purpose

    This charter establishes the Department of Energy Headquarters Information Technology Configuration Management Control Board (HQ IT CCB) and defines its scope of authority, membership, and responsibilities.

2. Scope

    The HQ IT Configuration Control Board (CCB) is established with the authority and responsibility for ensuring that all changes to the DOE HQ IT architecture will not adversely impact the operation of any existing system or subsystem. A System Change Proposal (SCP), consisting of either (or both) hardware configuration items (HWCIs) or software configuration items (SWCIs) or the appropriate program level and HQ level system baselines are the primary change instruments to be reviewed.

    2.1 Level of Review

Only changes that are a major departure from an existing operational architecture, such as:
   *   Upgrading from Novell 4.x to Novell 5.x,
   *   Migrating from Novell x.x with Microsoft NT x.x,
   *   Domain Name Services (DNS) reconfiguration,
   *   Implementation of a network intensive service (e.g., SMS)
require full CCB review and approval. Other, less major, changes should be submitted for information as a means of keeping the HQ IT baseline data current and valid.

3. Authority

    The HQ IT CCB derives its authority from the Chief Information Officer (CIO) and the HQ IT Collaboration Group. The CCB will review each SCP against its real or perceived impact on existing services and operations. The CCB has final authority over all issues brought before it for review. CCB decisions are documented in CCB minutes, and are implemented within the scope of its authority.

    CCB responsibilities include:

   *   The review and disposition of proposed modifications to current baselines,
   *   The review, prioritization, assignment of due dates and disposition for SCP's evaluation;
   *   Ensuring that introduction of the change will not have a negative impact on current operations;
   *   Approving SCP implementation schedules, and;
   *   Approval of updated baselines and documentation

4. Membership and Responsibilities

The CCB consists of the CCB Chairperson and the CCB Voting Members with administrative support provided by the CCB Secretariat.

4.1 CCB Chairperson

The DOE CIO shall appoint the CCB Chairperson. The Chairperson has the following responsibilities:

- Approves the CCB Agenda, including determination of agenda items.
- Facilitates the CCB decision process for disposition of SCP's brought before the board, within the scope of its authority. Decisions may be to approve, disapprove, defer, or send proposed changes back to the originator for rework.
- Ensures that originators of proposed changes are informed of decisions concerning disposition.
- Directs infrastructure and Corporate system change implementation, including schedules.

4.2   CCB Members

4.2.1   Standing Members

CCB Membership consists of all Headquarters IT Collaboration Group elements affected by any proposed change(s). Depending upon the magnitude of the change, this can be a single organization or multiple organizations.

4.2.2   Voting Members

Voting members will consist of the CCB Chairperson, the three Lead Program Secretarial Office members and five other Program Office members of the Headquarters IT Collaboration Group, as follows:

CCB VOTING MEMBERSHIP	
ORG	**Status**
CIO/OPS	**Chairperson**
DP	Voting Member
EE	Voting Member
EH	Voting Member
EM	Voting Member
FE	Voting Member
NE	Voting Member
RW	Voting Member
SC	Voting Member

4.2.3   Member Responsibilities

The read ahead materials and analysis supplied by the CCB Technical Review Group (defined below) will provide indicators delineating the impacts of the proposed change and the organizations affected by those impacts. CCB Members have the following responsibilities:

- Attend CCB meetings as scheduled, or send a designated representative with delegated authority to commit the organization being represented.
- Review all proposed changes on the agenda before the meeting and prepare an impact assessment, as appropriate, indicating the impact of the proposed change on current operations.
- Participate in the CCB discussions and decision making pertaining to the issues being addressed.

A CCB Technical Review Group (TRG), will analyze, develop alternatives, and make recommendations to the CCB for resolving issues in baseline change management documentation assigned for review. The TRG will perform in-depth technical review of change proposals to maintain compatibility and interoperability. The TRG, consisting of two DOE IA representatives, one of which represents Departmental Information Architecture and Standards, and no more than one each of a Software, Hardware and Network Engineer representing the major IM contractors at Headquarters. The major IT contractors supporting the HQ IT Collaboration Group organizations will each provide representatives to ensure appropriate resources within the organization reviewing and assessing the SCP's. This will give an independent and unbiased review and impact analysis of any proposed change(s). The results of this analysis will be provided to the *CCB Secretariat before* the regularly scheduled meetings.

4.3 CCB Secretariat

The CCB Secretariat shall be appointed by the CCB Chairperson and is responsible for CB administrative functions. The Secretariat coordinates CCB preparations and activities to assure that the board is prepared for meetings and that all actions are recorded. The CCB Secretariat has the following responsibilities:

- Coordination of meeting schedules and agendas with the CCB Chairperson
- Publication and distribution of CCB agendas.
- Preparation and distribution of change packages to the Chairperson and Members in advance of the meeting.
- Recording, publication and distribution of CCB minutes to the DOE HQ IT community.
- Tracking and maintaining the status of changes.
- Performing other support functions as directed by the CCB Chairperson.

5. Protocols

CCB meetings will be held at the direction of the CCB Chairperson, as needed, but will normally be held monthly. The CCB Chairperson can schedule emergency meetings within one week of the requestor's notice. Agendas will be distributed as approved by the CCB Chairperson. Items not contained in the agenda may be discussed, at the discretion of the Chairperson.

The CCB Secretariat will record pertinent information, including Members in attendance and decisions/actions associated with each proposed change. CCB minutes from the previous meeting will typically be distributed at the following meeting.

Change packages will be distributed to Members as soon as possible before a scheduled meeting. Disposition direction detailing the actions decided upon for each proposed change will be recorded in the minutes by the CCB Secretariat, and monitored for implementation. Action items assigned at CCB meetings will be monitored by the Chairperson to assure timely closure.

6. Implementation Procedures

Operating Overview: The Department of Energy Headquarters Information Technology Configuration Management Control Board (HQ IT CCB) will serve as the configuration management forum considering baseline changes and (systems) operations issues.

All System Change Proposals (SCP) preparation and processing, together with distribution of minutes, documents, and other program-related information, will take place using the on-line web server:

([http://nmic.doe.gov/scp/).](http://nmic.doe.gov/scp/)."

Configuration Management Cycle: The (HQ IT CCB) meetings will be scheduled as required during the month/year. Meetings will be scheduled to support the needs of the operational user and to comply with baseline implementation schedules.

System Change Proposal (SCP) preparation and processing: A SCP will contain an analysis of impact from the perspective of the submitting group or Agency. Evaluations of the SCP's by each subgroup of the Technical Review Group (TRG) will contain impact analyses from a technical and an operational perspective. They will include information on proposed time frame for implementation, effect on automated systems, changes required to user publications, etc., as applicable.

Format: A SCP will be prepared in a standard electronic format (see sample below). The originators will assign precedence to SCP's in accordance with CCB Charter. Priority SCP's will be designated when expedited administrative handling and staffing is required; e.g., SCP's having special operational expediting requirement. Urgent SCP's will be so designated when an immediate operational requirement exists. Rationale supporting this designation will accompany the SCP.

Fast Track Approval: Electronic, telephone or other voting procedures may be used for proposed changes considered by the originator to be non-controversial, or where advance coordination indicates probable acceptance. Electronic voting can also use the web server:

http://nmic.doe.gov/scp/

Changes to be voted on by electronic means, will be distributed in the same manner as those requiring a CCB meeting, except that a cover letter will request that each CCB member provide a position on the change proposal electronically to the CCB secretary. If no problems are identified and a unanimous vote is obtained, with no member requesting that a technical review TRG be convened, the change will be considered agreed and a CCB document will be issued without the need for a CCB meeting. Administrative/wording corrections are not sufficient cause to require a formal CCB meeting. However, administrative and wording corrections collected electronically must be distributed to other CCB member representatives prior to concluding an electronic vote.

7   Rules for Decision Process

1.   The chairperson may vote only to break ties.
2.   Any voting member of the CCB, including the chairperson, may declare a CCB decision a substantive issue. This must be done prior to the end of the meeting, except when voting member requests a delay period because significant new information was uncovered at the meeting. In this case, that member has five working days from the end of the meeting to declare, in writing to the CCB chairperson and other CCB members, the CCB decision as a substantive issue.
3.   The member declaring a CCB decision as a substantive issue will forward their position within ten work days from date of the declaration to the chairperson, Standards Coordinating Committee, for standards issues, and to the chairperson of the TRG for operational and technical issues for a decision or further action. The member declaring a CCB decision as a substantive issue will provide information copies of all information pertinent to their position to all CCB members.
4.   Once announced, notification of decisions on issues forwarded to the Standards and TRG the chairpersons will be disseminated, by using electronic means, to all CCB members.
5.   When required by majority vote, the CCB chairperson shall defer a change proposal for rework/revision, etc., and resolution at a future CCB meeting. When a change proposal is revised or reworked, it will be rescheduled for another review and evaluation by all CCB members.
6.   A SCP will be deferred at the request of any CCB member at its first consideration by the CCB. It will also be deferred if it is not contained on the published agenda. A SCP so deferred may be scheduled for consideration at the next scheduled CCB meeting for a vote using electronic voting procedures.
7.   The final agreed disposition of each SCP considered by the CCB will be documented and prepared by the (HQ IT CCB) secretary and signed by the CCB chairperson. This document is the instrument by which the SCP becomes part of the HQ IT baseline. It provides the final disposition of the SCP and records the member's votes.

8. This CCB document will indicate the implementation date at which time the requestor can be expected to apply the information contained in the SCP to their respective systems.

Headquarters
System Change Proposal (SCP)

DOE POC: **Date:**

System Integration POC: **Projected Baseline Date:**

Based Upon Baseline Version:

SCP Priority: Emergency: ___   Urgent: ___ Routine: ___

Brief Description of SCP:

DOE Infrastructure Impact:

Summary of Proposed Baseline Changes:

Summary of Hardware Changes

Summary of Software Changes:

Logistics:

Major Milestones:

Project Outline:

Summary of Security Impacts on the DOE Network as a Whole:

Identification of Relationships between Related DP Projects/Systems:

Approved by CCB(date approved):

Deferred for: